MASTER OF SCIENCE
IN
COMPUTER SCIENCE

IMPLEMENTATION OF A NETWORK ADDRESS TRANSLATION MECHANISM OVER IPV6

Trevor J. Baumgartner-Ensign, United States Navy
B.S., United States Naval Academy, 2003
Master of Science in Computer Science-June 2004
Matthew D.W. Phillips-Ensign, United States Navy
B.S., United States Naval Academy, 2003
Master of Science in Computer Science-June 2004
Advisors: Cynthia Irvine, Department of Computer Science
Thuy D. Nguyen, Department of Computer Science

Network Address Translation (NAT) for Internet Protocol Version Four (IPv4) was developed primarily to curb overcrowding of the Internet due to dwindling global IP addresses; however, NAT provides several other benefits. NAT can be used to mask the internal IP addresses of an Intranet. IPv6, the emerging standard for Internet addressing, provides three times the number of bits for IP addressing. While IPv6 does not need NAT for connectivity, other NAT features such as address hiding are valuable. There is currently no NAT implementation for IPv6.

The focus of this research was the design and development of a NAT implementation for IPv6. This implementation will be used within a multilevel testbed. In addition, the NAT implementation developed here can facilitate the Department of Defense (DoD) transition to IPv6, planned for 2008, by providing services currently not available for IPv6.

A working implementation of NAT for IPv6 within the Linux kernel has been produced. The NAT development created here has been tested for support of the protocols of Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP) for IPv6.

KEYWORDS: Network Address Translation, NAT, IPv6, IPv4, MYSEA, MLS, Common Criteria, Linux Source Code, Netfilter, Iptables

CYBERCIEGE SCENARIO ILLUSTRATING SECRECY ISSUES THROUGH MANDATORY AND DISCRETIONARY ACCESS CONTROL POLICIES IN A MULTI-LEVEL SECURITY NETWORK

Robert L. LaMore-First Lieutenant, United States Air Force
B.S., Austin Peay State University, 1997
Master of Science in Computer Science-June 2004
Advisors: Cynthia Irvine, Department of Computer Science
Paul Clark, Department of Computer Science
Second Reader: Michael Thompson, Department of Computer Science

User training in computer and network security is crucial to the survival of modern networks, yet the methods employed to train users often seem ineffective. One possible reason is that users are not fully engaged during these training sessions and thus they tend to forget the lessons being taught.

The CyberCIEGE game introduces a new method of training in computer and network security. The player engages in a simulation-based network security game that reflects real-world security principles. Each time the CyberCIEGE game runs, it loads a *Scenario Definition File (SDF)* written to teach specific security concepts.

This thesis developed such a scenario definition file for the CyberCIEGE game. The educational purpose of the scenario is to illustrate secrecy issues in the context of mandatory and discretionary access control in a multilevel networked environment. The primary work of this thesis is to construct the scenario definition file such that playing the resulting game achieves this educational purpose.

This thesis also constructs scenario definition files to test the CyberCIEGE game engine for expected results. These tests provide support for several recommendations for improvement in the game engine.

KEYWORDS: Information Assurance, CyberCIEGE, Scenario Definition File, Network Security Training

EXPLORING A CHROMAKEYED AUGMENTED VIRTUAL ENVIRONMENT FOR VIABILITY AS AN EMBEDDED TRAINING SYSTEM FOR MILITARY HELICOPTERS

Mark J. Lennerton-Captain, United States Marine Corps
B.S., Keene State College, 1990
Master of Science in Computer Science-June 2004
Advisor: Rudolph P. Darken, Department of Computer Science
Second Reader: CDR Joseph Sullivan, USN, Department of Computer Science

Once the military helicopter pilot deploys aboard a Naval vessel, all training platforms, short of the actual aircraft, that present enough fidelity to maintain the highest levels of readiness are left behind. This thesis takes a preliminary step in creating a trainer that places the pilot in an immersive and familiar environment to exercise myriad piloting tasks as faithfully and as rigorously as in actual flight. The focus of this thesis is to assess the viability of a chromakeyed augmented virtual environment (ChrAVE) trainer embedded in a helicopter for use in maintaining certain perishable skills. Specifically, this thesis addresses the task of helicopter low-level land navigation. The ChrAVE is developed to substantiate the viability of having embedded trainers in helicopters. The ChrAVE is comprised of commercial-off-the-shelf (COTS) equipment on a transportable cart. In determining whether a system such as the ChrAVE is viable as a laboratory for continued training in a virtual environment, the opinion of actual pilots that are tasked with realistic workloads is used. Additionally, empirical data is collected and evaluated according to the subject pool's thresholds for acceptable low-level navigation performance.

KEYWORDS: Virtual Environments, Terrain Association, Navigation, Embedded Trainers, Chromakey, Augmented Reality, Mixed Reality, Helicopter, Mission Rehearsal, Route Rehearsal, Spatial Orientation, Motion Tracked, Human-computer Interface

SUITABILITY OF THE SRC-6E RECONFIGURABLE COMPUTING SYSTEM FOR GENERATING FALSE RADAR IMAGES

Kendrick R. Macklin-Lieutenant, United States Navy
B.S., San Diego State University, 1997
Master of Science in Computer Science-June 2004
Advisor: Neil Rowe, Department of Computer Science
Second Reader: Douglas J. Fouts, Department of Electrical and Computer Engineering

This thesis evaluates the usefulness of the SRC-6E reconfigurable computing system for a radar signal processing application and documents the process of creating and importing very high speed integrated circuit hardware description language (VHDL) code to configure the user definable logic on the SRC-6E. The research builds on previous work which implemented a false radar imaging algorithm on the SRC-6E. Data from alternative computational approaches to the same problem are compared to determine the effectiveness of SRC-6E solution. The results show that the SRC-6E provides and effective solution for implementations with greater than 64 range bins. An evaluation of the SRC-6E difficulty of use is conducted, including a discussion of required skills, experience, and development times. The algorithm test code is included in the appendices.

KEYWORDS: Benchmark, Reconfigurable Computing, VHDL, SRC-6E, FPGA, False Radar Target Synthesis

A CYBERCIEGE SCENARIO ILLUSTRATING MULTI-LEVEL SECRECY ISSUES IN AN AIR OPERATIONS CENTER ENVIRONMENT

Marc K. Meyer-Captain, United States Air Force
B.S., Norwich University, 1999
Master of Science in Computer Science-June 2004
Advisors: Cynthia Irvine, Department of Computer Science
Paul Clark, Department of Computer Science
Second Reader: Michael Thompson, Department of Computer Science

CyberCIEGE provides an addition to traditional Information Assurance (IA) education in the form of an interactive, entertaining, commercial-grade, PC-based computer game. Educational sessions are contained in scenarios that serve to teach particular IA concepts. The details of a scenario are contained in a Scenario Definition File (SDF), which is written in the CyberCIEGE Scenario Definition Language. This language is rich enough to express a range of information security policies and operational data access requirements, resulting in a near limitless pool of possible scenarios.

This thesis develops a playable scenario illustrating confidentiality protection concepts in an open storage environment modeled after an Air Operations Center. Educational goals include physical protection of high value assets and use of strong authentication policies to protect moderate value assets. The major work of this thesis is design of an SDF to reflect a military information security policy and work flow environment contained in the educational goals. The confirmation of the proper operation of selected aspects of the CyberCIEGE game engine, and the assurance that the SDF confronts the player with the security trade-offs, occur through the application of a testing methodology. The creation of detailed solutions and examples of incorrect gameplay choices facilitate this testing.

KEYWORDS: CyberCIEGE, Information Assurance, IA, Scenario Definition File, SDF

SECURE REMOTE NETWORK ADMINISTRATION AND POWER MANAGEMENT

Mark P. Sullivan-Captain, United States Air Force
B.S., University of Maryland University College, 2000
Master of Science in Computer Science-June 2004
Advisor: Dale Courtney, Department of Information Sciences
Second Reader: Dennis Volpano, Department of Computer Science

Remote Network Administration allows network administrators to manage their networks while being physically separated from the network equipment. Having the capability to manage wired and wireless networks securely, from remote locations, can substantially reduce operating expenses across the entire Department of Defense. A variety of methods for remotely managing networks is explored for both wired and wireless networks. Requirements for remote network administration are identified. Chief among them is security and the ability to remotely manage power. Several widely-used remote management utilities are examined. All fail to meet these two requirements. A new power control device is presented that can be managed securely and remotely.

KEYWORDS: Remote Network Administration, Network Management, Power Management

EFFECTIVE USE OF JAVA DATA OBJECTS IN DEVELOPING DATABASE APPLICATIONS. ADVANTAGES AND DISADVANTAGES

Paschalis Zilidis-Major, Hellenic Air Force
B.S., Hellenic Air Force Academy, 1988
Master of Science in Computer Science-June 2004
Advisor: Thomas Otani, Department of Computer Science
Second Reader: Arijit Das, Department of Computer Science

Currently, the most common approach in developing database applications is to use an object-oriented language for the front end module, and a relational database for the back end datastore. The major

disadvantage of this approach is the well-known “impedance mismatch,” in which some form of mapping is required to connect the objects in the front end and the relational tuples in the back end.

Java Data Objects (JDO) technology is recently proposed Java applications program interface (API) that eliminates the impedance mismatch. By using JDO API, the programmers deal strictly with objects. JDO hides the details of the backend datastore by providing the object-oriented view of the datastore. JDO automatically handles the mapping between the objects and the underlying data in the relational database, which is hidden from the programmer.

This thesis investigates the effectiveness of JDO. Part of the analysis develops a database application using JDO. Although JDO provides the benefits of object-orientation in design and implementation of the databases, it is not immune to problems and limitations. The thesis also analyzes the advantages and disadvantages of using JDO and discusses the areas requiring improvements in future releases.

KEYWORDS: Datastore, Java Data Objects, JDO, API, Java